

AO 106 (Rev. 04/10) Application for a Search Warrant

**United States District Court**  
for the  
Western District of New York

In the Matter of the Search of

*(Briefly describe the property to be searched or identify the person by name and address.)*

Case No. 22-MJ-732-MJP

A gray colored 2018 Honda CRV, containing "Roc City" decals, with New York State Registration "16108LY" and Vehicle Identification Number (VIN): 7FARW2H52JE041853; 703 Webster Road, Webster, New York; and the person of ASHLEY JACKSON, DOB: 08/30/1988, SSAN: XXX-XX-6483, including any clothing or bags in her immediate control, more fully described in Attachments A-1, A-2 and A-3.

**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property located in the Western District of New York *(identify the person or describe the property to be searched and give its location)*: A gray colored 2018 Honda CRV, containing "Roc City" decals, with New York State Registration "16108LY" and Vehicle Identification Number (VIN): 7FARW2H52JE041853; 703 Webster Road, Webster, New York; and the person of ASHLEY JACKSON, DOB: 08/30/1988, SSAN: XXX-XX-6483, including any clothing or bags in her immediate control, more fully described in Attachments A-1, A-2 and A-3.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B, Schedule of Items to be Seized, which attachment is incorporated by reference as if fully set forth herein, all of which are fruits, evidence and instrumentalities of a violation of Title 18, United States Code, Sections 1035 & 1347.

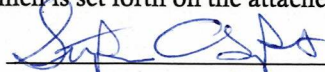
The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 2252A(a)(2)(A) & 2252A(a)(5)(B).

The application is based on these facts: *See attached affidavit.*

- ☒ continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

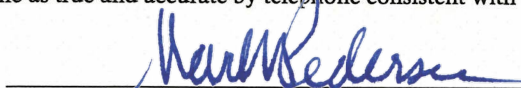
Stephen Csapo, S/A FBI

Printed name and title

Application submitted by email/pdf and attested to me and before me as true and accurate by telephone consistent with Fed.R.Crim.P. 4.1 and 41(d)(3)

Date: December 12, 2022

City and state: Rochester, New York



Judge's signature

Hon. Mark W. Pedersen, U.S. Magistrate Judge

Printed name and Title

**ATTACHMENT A-1**

THE SUBJECT VEHICLE is described as a gray colored 2018 Honda CRV, containing “Roc City” decals, with New York State Registration “16108LY” and Vehicle Identification Number (VIN): 7FARW2H52JE041853. A photo of THE SUBJECT VEHICLE is depicted below.



**ATTACHMENT A-2**

THE SUBJECT RESIDENCE is located at 703 Webster Road, Webster, New York. THE SUBJECT RESIDENCE is a two-story single-family residence. The exterior appears to be a white colored siding with red colored shutters. The number “703” appears in black numbering affixed to the residence near the driveway. A photo of THE SUBJECT RESIDENCE is depicted below.





**ATTACHMENT A-3**

THE SUBJECT PERSON is ASHLEY JACKSON ("JACKSON"), DOB: 08/30/1988, SSAN: XXX-XX-6483, including any clothing or bags in her immediate control. JACKSON is approximately 6'00" and weighs approximately 260-280 pounds. JACKSON's photo is attached.



**ATTACHMENT B**

1. All records relating to violations of 18 U.S.C. § 1035 (False Statements Relating to Health Care Matters), and § 1347 (Health Care Fraud) (the “Specified Federal Offenses”), including:

- a. Records relating to the operation, control, and/or use of the name of the following business: Roc City Transport
- b. Records relating to any business operated by Ashley Jackson.
- c. Bank statements, bank checks, cash receipts, money transfer records and receipts, money remittance instructions, customer information and records, sales records, ledgers showing cash and checks received, contracts, fax records, correspondence, including but not limited to correspondence with others regarding the transmission of money, printed emails, letters, faxes, and telephone logs or messages that constitute evidence of the Specified Federal Offenses;
- d. Address and/or telephone books, Rolodex indices, invoices, communications, and any papers or records reflecting names, addresses, email addresses, telephone numbers, pager numbers, facsimile numbers and/or telex numbers of co-conspirators, financial institutions, and other individuals or businesses with whom a financial relationship exists;
- e. Books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashier's checks, bank checks, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, secreting, transfer, concealment and/or expenditure of money;
- f. United States currency, digital currency such as Bitcoins stored on electronic wallets or other means, and records relating to income derived from the Specified Federal Offenses and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, checkbooks, check registers, securities, precious metals, jewelry, antique or modern automobiles, including stocks or bonds in amounts indicative of the proceeds of the Specified Federal Offenses;
- g. All records relating to MAS, trip sheets, EMedNY, and records related to Medicaid Recipients ROC CITY billed services for.
- h. Cellular telephones (including searching the memory thereof) and used to generate, transfer, count, record and/or store the information and evidence described in this Attachment;
- i. Photographs, records, and documents, including still photographs, negatives, video tapes, films, undeveloped film and the contents therein, slides, and any video, recording or photographic equipment containing the aforementioned items,

containing information regarding the identities of coconspirators or those involved in the Specified Federal Offenses;

- j. Indicia of occupancy, residency, ownership and/or use of the subject premises, including but not limited to, utility and telephone bills; canceled envelopes; rental, purchase or lease agreements; and keys;
  - k. Articles of Incorporation, corporate resolutions, corporate minute books, corporate stock books, corporate stock certificates, corporate state charters, records of corporate franchise taxes paid, corporate financial statements, profit and loss statements, balance sheets, and statements of cash flow;
  - l. General journals, cash receipt journals, cash disbursement journals, sales journals and computer printout sheets;
  - m. General ledgers and subsidiary ledgers including notes receivables, accounts receivables, accounts payable, notes payable, adjusting journals and closing ledgers;
  - n. Receipts and invoices for all expenditures;
  - o. All Federal income tax returns, Forms 1040, W-2, 1099, 1120, 940, 941, K-1 , or copies of same and supporting work papers, summary sheets, and analyses used in the preparation of the tax returns
  - p. Records relating to the solicitation, contracting, negotiating, or closing of any loan agreement;
  - q. Records of payments made in connection with the Specified Federal Offenses; and
  - r. All personal financial statements, contact bids, proposals, closing statements, warranty deeds of trust, release deeds, or other documentation supporting conveyances and/or ownership of properties, and vehicle registration and titles; and
  - s. Safes, key-lock strong boxes, suitcases, locked cabinets, and other types of locked or closed containers used to secrete and store currency, books, records, documents, financial instruments, and other items of the sort described above. Law enforcement officers executing this Warrant are specifically authorized to open any such locked safes or containers including, where necessary, by using force.
2. Computers, cellular telephones, and/or storage media used as a means to commit the Subject Offenses. For any computer, cellular telephone, and/or or storage medium whose seizure is otherwise authorized by this warrant, and any computer, cellular telephone, and/or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER")
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of any COMPUTER described herein, law enforcement personnel are authorized to press the fingers (including thumbs) of Jackson to the devices, and to any fingerprint sensors on those devices or applications therein, for the purpose of attempting to unlock the COMPUTER in order to search the contents as authorized by this warrant. Law enforcement are further authorized to hold any COMPUTER found at the premises in front of the face of Jackson to activate the facial recognition feature; and/or (3) hold the Device(s) found at the premises in front of the face of Jackson to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.



IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF NEW YORK

---

IN THE MATTER OF THE SEARCH OF THE SUBJECT LOCATIONS AS MORE  
PARTICULARLY DESCRIBED IN ATTACHMENTS A-1, AND A-2.

---

**AFFIDAVIT IN SUPPORT OF APPLICATIONS UNDER RULE 41 FOR  
WARRANTS TO SEARCH AND SEIZE**

I, Stephen J. Csapo, Special Agent of the Federal Bureau of Investigation (FBI),  
being duly sworn, depose and state that:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search three locations further described in Attachments A-1, A-2, and A-3 for things described in Attachment B-1. The three locations are as follows:

- Gray 2018 Honda CRV, With New York State Registration 16108LY and VIN: 7FARW2H52JE041853 (THE SUBJECT VEHICLE).
- 703 Webster Road, Webster, New York 14580 (THE SUBJECT RESIDENCE).
- The person of ASHLEY JACKSON ("JACKSON"), DOB: 08/30/1988, SSAN#XXX-XX-6483 (THE SUBJECT PERSON)

2. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and have been so employed since September of 2015. I am currently assigned to the Buffalo, New York Field Office. My experience as an FBI Special Agent has included the investigation of cases involving corporate fraud, investment fraud, health care fraud, bank fraud, money laundering, public corruption, cases involving computer

intrusions and cases involving the use of computers to commit crimes. I have received training and have gained experience in interview and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. The information contained in this Affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part, and any dates, dollar amounts, and times referenced in this affidavit are "on or about" that date, amount, or time, and are approximate.

#### **THE SUBJECT LOCATIONS**

4. The locations to be searched are specifically described, and their photographs are contained, in Attachments A-1, A-2, and A-3 to the applications to obtain the corresponding search warrants. They are more particularly described below.

5. THE SUBJECT VEHICLE is a 2018 Honda CRV SUV, bearing New York State Registration 16108LY, which is registered to ROC CITY TRANSPORT (hereinafter "ROC CITY"), 703 Webster Road, Webster, New York 14580 (THE SUBJECT RESIDENCE). A photo of THE SUBJECT VEHICLE is enclosed in Attachment A-1.

6. THE SUBJECT RESIDENCE is a two-story single-family residence. The exterior appears to have a white colored siding and red colored shutters. The number "703" appears on the front of the residence in black numbering. A photo of THE SUBJECT RESIDENCE is enclosed in Attachment A-2.

7. THE SUBJECT PERSON is ASHLEY JACKSON ("JACKSON"), DOB: 08/30/1988, SSAN#XXX-XX-6483, including any clothing or bags in her immediate

control. JACKSON is approximately 6'00" and weighs approximately 260-280 lbs. A photo of THE SUBJECT PERSON is contained in Attachment A-3.

8. Based on the facts and circumstances of this investigation, as set forth below, there is probable cause to believe that ASHLEY JACKSON (JACKSON), and others not yet known, have committed, are committing, and will continue to commit violations of federal law involving False Statements Relating to Health Care Matters in violation of Title 18, United States Code 1035, and Health Care Fraud in violation of Title 18, United States Code 1347 (TARGET OFFENSES).

9. Additionally, based upon the investigation in this case, there is probable cause to believe that JACKSON is using THE SUBJECT VEHICLE and THE SUBJECT RESIDENCE in connection with the commission of the TARGET OFFENSES. There is also probable cause to believe that the items set forth in Attachment B, which constitute evidence, fruits, and/or instrumentalities of violations of the Specified Federal offenses, and other federal crimes, are currently located and concealed at THE SUBJECT RESIDENCE and THE SUBJECT VEHICLE. As such, authority is sought to search THE SUBJECT RESIDENCE and THE SUBJECT VEHICLE for items enumerated in Attachment B. Authority is further sought to search the entire premises of THE SUBJECT RESIDENCE and THE SUBJECT VEHICLE, including any locked containers, safes, filing cabinets, stationary and moveable containers, where the items specified in Attachment B may be found, and to seize all of the items listed in Attachment B as evidence, contraband, fruits, and instrumentalities of the TARGET OFFENSES.

#### **BACKGROUND: The Medicaid Program**

10. The Medicaid program is a federal and state health care program that provides health care benefits to individuals and families who meet specified financial and other eligibility requirements, and certain other individuals who lack adequate resources to pay for medical care. It is a "health care benefit program" and "federal health care program" as defined by 18 U.S.C. 24(b) and 42 U.S.C. 1320a-7b(f), respectively. The Centers for Medicare and Medicaid Services, a federal agency under the United States Department of Health & Human Services, is responsible for overseeing the Medicaid program in New York State. An

individual who receives benefits under Medicaid is referred to as “beneficiary”.

11. Under the Medicaid transportation subsidy, if a beneficiary does not have, or cannot afford, suitable transportation to a medical appointment, Medicaid will pay for the beneficiary to travel to and from the medical appointment via a private transportation company, such as a taxi-cab company. After the ride has been performed, the private transportation company, rather than the beneficiary, is responsible for billing Medicaid for the cost of the transportation. For any given trip, a Medicaid payment to a transportation company is in part determined by the total distance that the beneficiary is transported; a roundtrip results in a higher payment to a company than a one-way trip, for example. In order to receive payment, a transportation company must attest to the accuracy of each trip.

12. In order to schedule a Medicaid transportation trip, beneficiaries call MAS, a New York State contractor based in Syracuse, New York. A beneficiary can generally specify which transportation company he/she prefers to be picked up by. A beneficiary can also have a regularly scheduled transportation appointment with the same company. For instance, the same company may bring a beneficiary to and from a recurring weekly appointment; this is often referred to as a “standing order.”

13. In order to be reimbursed following the provision of Medicaid transportation services, a transportation company must attest to MAS that they actually provided the requested ride services to the beneficiary or beneficiaries. These attestations are made electronically via the internet and MAS keeps a copy of these attestations. The transportation company then submits those attested trips to Medicaid for reimbursement.

#### **GPS Tracker Search Warrants**

14. Between October 21, 2022 and December 9, 2022, law enforcement executed 3 GPS tracker search warrants which collected ROC CITY information. The GPS trackers confirmed that ROC CITY is engaging in health care fraud in the two ways mentioned above. First, ROC CITY is attesting to, and being reimbursed for, Medicaid transportation trips that are not actually being performed. Second, ROC CITY is improperly attesting that group rides were performed as individual rides.

15. An example of the first fraud is as follows: Between October 27, 2022 and December 9, 2022, a GPS tracker was placed on THE SUBJECT VEHICLE. According to MAS records, JACKSON attested that JACKSON used THE SUBJECT VEHICLE to perform 6 round-trip Medicaid rides between November 14, 2022 and November 23, 2022, purportedly driving a Medicaid Recipient 1 (MR-1) who happens to be JACKSON's spouse that resides with her at THE SUBJECT RESIDENCE, to a physical therapy appointment at 4901 Lac Deville Boulevard, Rochester, New York. The GPS data showed that THE SUBJECT VEHICLE did not travel in the vicinity of MR-1's appointments on those dates. Additionally, CCTV cameras in the vicinity of THE SUBJECT RESIDENCE show that JACKSON and MR-1 did not depart THE SUBJECT RESIDENCE together on those dates. Yet, JACKSON attested in MAS that she transported MR-1 in THE SUBJECT VEHICLE to the above-mentioned appointments and was paid approximately \$739.83.

16. Another example of the first fraud is as follows: Between October 27, 2022 and December 9, 2022, a GPS tracker was placed on THE SUBJECT VEHICLE. According to MAS records, JACKSON attested that JACKSON used THE SUBJECT VEHICLE to perform 14 round-trip Medicaid transportations between October 27, 2022 and November 29, 2022, purportedly driving a Medicaid Recipient (MR-2), to and from a Methadone clinic at 2613 West Henrietta Road, Rochester, New York. The GPS data showed that JACKSON did not perform these transportations and the GPS tracker did not travel near the vicinity of MR-2's residence during the relevant time period. Yet, JACKSON certified that she transported MR-2 from MR-2's residence to the Methadone clinic using THE SUBJECT VEHICLE and was paid approximately \$1,865.92.

17. Regarding the second type of fraud, wherein ROC CITY billed for group rides as if they were individual rides, the GPS tracker records also showed a consistent pattern with JACKSON using THE SUBJECT VEHICLE. Between October 27, 2022 and December 9, 2022, a GPS tracker was placed on THE SUBJECT VEHICLE and physical surveillance was performed on THE SUBJECT VEHICLE. The surveillance confirmed that in several rides performed by ROC CITY in THE SUBJECT VEHICLE and another vehicle (2019 Toyota Corolla) registered to ROC CITY, there were multiple individuals, in addition to the driver, in the vehicles that were driven to Methadone clinics. Once the vehicles arrived at the



Methadone clinics, all occupants, excluding the driver, exited the vehicle and went into the Methadone clinic. They were then driven back to the same locations they came from. MAS records showed that during these same time frames, ROC CITY was attesting to and billing for rides as if they were performed as individual rides and not group rides.

18. For example, on August 5, 2022, the writer was conducting surveillance on THE SUBJECT VEHICLE to observe transportations. THE SUBJECT VEHICLE approached an address in Rochester, New York and Medicaid Recipient 3 (MR-3) entered the vehicle. THE SUBJECT VEHICLE was then observed traveling in the vicinity of Medicaid Recipient 4's (MR-4) address in Rochester, New York. Moments later, MR-3 and MR-4 were observed exiting THE SUBJECT VEHICLE and entering a Methadone clinic at 2613 West Henrietta Road, Rochester, New York. MAS records showed that ROC CITY attested to both rides as if they were driven individually to the Methadone clinic, resulting in a higher reimbursement for the transportation to ROC CITY.

#### **MR-2 Interview**

19. On or about December 1, 2022, MR-2 was interviewed by your affiant in person in Rochester, New York.

20. During this interview, MR-2 stated he and his significant other, who is also a Medicaid Recipient (MR-5), were often transported together in THE SUBJECT VEHICLE by JACKSON and also transported together in another ROC CITY vehicle by one of JACKSON's drivers. Additionally, during the interview, MR-2 stated he drives MR-2 and MR-5 to the Methadone clinic personally. JACKSON sends a text message to MR-2 and MR-5 the evening before a scheduled transportation to see if MR-2 and MR-5 do in fact need transportation. MR-2 stated if he personally drives to the appointment he is often reimbursed by JACKSON through Cash App.

21. Specifically, on or about November 28, 2022, JACKSON sent a text message to MR-2 stating "Did you guys need a ride tomorrow or you driving". MR-2 responded to JACKSON stating "I can drive for (emoji – gas and money bag)". JACKSON responds "Ok I'll be Able to send it later tonight". A review of the Cash App account for MR-2 showed that

the next morning, November 29, 2022, JACKSON sent a \$25.00 transfer to MR-2. JACKSON later attested to transporting MR-2 and MR-5 on November 29, 2022, receiving compensation from Medicaid of \$225.34 (\$133.28 for MR-2 and \$92.06 for MR-5). MR-2 and MR-5 attested to your affiant that the transportation did not occur on November 29, 2022 from ROC CITY, which is consistent with GPS tracker data on THE SUBJECT VEHICLE and CCTV surveillance on THE SUBJECT RESIDENCE.

#### **ROC CITY Business Address**

22. The registered business address for ROC CITY is THE SUBJECT RESIDENCE and has been since ROC CITY was established in August of 2017 in the State of New York.

23. In March 2020, ROC CITY applied for a loan through the Small Business Administration (SBA) Economic Injury Disaster Loan (EIDL) program. On the application, JACKSON listed THE SUBJECT RESIDENCE as the business location for ROC CITY and listed JACKSON as the 100% owner of ROC CITY.

24. Bank records for ROC CITY were reviewed for the period January 1, 2018 to July 28, 2022. At the time of opening, JACKSON lists THE SUBJECT RESIDENCE as the business address for ROC CITY. All of the statements contained during the relevant period list THE SUBJECT RESIDENCE as the mailing address.

**Probable Cause to Search THE SUBJECT RESIDENCE, 703 Webster Road, Webster, New York, THE SUBJECT PERSON, Ashley Jackson, and THE SUBJECT VEHICLE, a 2018 Honda CRV.**

25. Based on the above information, there is probable cause to believe JACKSON and ROC CITY are committing health care fraud. Further, there is probable cause to believe evidence of this fraud will be found at 703 Webster Road, Webster, New York, which is further described in Attachment A-2, in THE SUBJECT VEHICLE, which is further described in Attachment A-1, and on THE SUBJECT PERSON, which is further described in Attachment A-3.

26. As stated above, when the transportations are performed, Medicaid requires the taxi company (ROC CITY) to generate a document known as a "trip sheet." The trip sheet includes the date and time of the ride performed and is signed by the beneficiary and the driver. The information on the trip sheet is then entered into MAS and attested to by ROC CITY in MAS to facilitate the billing process. Medicaid regulations require transportation companies to keep these trip sheets for record-keeping purposes. Based on records known to investigators, the business location for ROC CITY is 703 Webster Road, Webster, New York, and has been since the company formation in 2017 and therefore the records are likely to be stored at this address. We expect that the trip sheets will show a discrepancy between the rides actually performed by ROC CITY and those billed to Medicaid, thus evidencing the alleged health care fraud.

27. Additionally, 703 Webster Road, Webster, New York is also where JACKSON resides. CCTV surveillance from the vicinity of THE SUBJECT RESIDENCE has shown THE SUBJECT PERSON come and go from THE SUBJECT RESIDENCE using THE SUBJECT VEHICLE. Surveillance has observed JACKSON transporting Medicaid Recipients using THE SUBJECT VEHICLE on numerous instances as described above and therefore it is likely that evidence of the TARGET OFFENSES may be found in THE SUBJECT VEHICLE since it was used in connection with the alleged fraud.

**Evidence Likely to be Present at THE SUBJECT RESIDENCE, THE SUBJECT VEHICLE, and on THE SUBJECT PERSON**

28. The requested warrants would authorize searches of the premises identified in Attachment A-2, the vehicle identified in Attachment A-1, and the person identified in Attachment A-3, including all structures on the premises and all electronic devices contained in or upon them.

29. The evidence in this investigation includes paper trip sheets that are signed by both the beneficiary and the driver. Other evidence in this investigation consists largely of electronically stored information, such as the attestations made on the internet in a New York based contractor website called MAS, and communications between THE SUBJECT PERSON and the various Medicaid Recipients. Based on my training and experience, I know

that this type of information may be – and frequently is – stored on small and readily portable devices, such as laptop computers, flash drives, external hard drives, and mobile devices.

30. As further discussed above, JACKSON, attested to these transportations in MAS causing reimbursements from Medicaid since in or around 2017. JACKSON used THE SUBJECT RESIDENCE as the main business address for ROC CITY and used the premises to store THE SUBJECT VEHICLE which was used in connection with the alleged fraud. Therefore, there is probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses will be found at THE SUBJECT RESIDENCE, THE SUBJECT VEHICLE, and on THE SUBJECT PERSON.

#### TECHNICAL TERMS

31. As described above and in Attachment B, this application seeks permission to search for records that might be found on the premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

32. *Probable cause.* I submit that if a computer or storage medium is found at THE SUBJECT RESIDENCE, THE SUBJECT VEHICLE, or on THE SUBJECT PERSON, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium

that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation, I am aware that computer equipment was used to generate, store, and/or print documents used in the fraud scheme. There is reason to believe that there is a computer system currently located on the premises.

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the



attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet

searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to create fraudulent documents, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime.

g. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

34. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to

make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it require considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

35. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-

assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

### **BIOMETRIC CHARACTERISTICS**

36. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

37. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

38. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

39. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

40. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

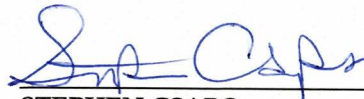
41. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter JACKSON with a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.



**SEALING ORDER REQUESTED**

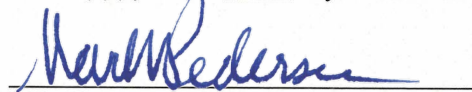
42. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this application, including the application, affidavit, and search warrants, and the requisite inventory notice (with the exception of the copy of the warrant and the inventory notice that will be left at THE SUBJECT RESIDENCE, THE SUBJECT VEHICLE, and with THE SUBJECT PERSON.) Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation, and premature disclosure of the contents of this affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

43. Based on the foregoing, I respectfully request that this Court issue search warrants for THE SUBJECT RESIDENCE, THE SUBJECT VEHICLE, and THE SUBJECT PERSON, more particularly described in Attachments A1, A2, and A3 authorizing the seizure of the items described in Attachment B.



STEPHEN CSAPO  
Special Agent, Federal Bureau of Investigation

Affidavit submitted electronically by email in .pdf format. Oath administered, and contents and signature attested to me as true and accurate telephonically pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on this 12th day of December 2022.



MARK W. PEDERSEN  
UNITED STATES MAGISTRATE JUDGE